Appendix I
National Security Information Inspections

I.1 REFERENCES

- Executive Order 13292, Further Amendment to Executive Order 12958, as amended, Classified National Security Information, March 25, 2003.
- Implementing Directive for E.O. 12958, 32 CFR Part 2004
- Information Security Oversight Office (ISOO) Directive 1

I.2 GUIDELINES ON HOW TO PREPARE FOR A NATIONAL SECURITY INFORMATION (NSI) INSPECTION.

A. Pre-Inspection Brief.

1. A pre-inspection briefing or a pre-inspection packet will be provided to the bureau or operating unit's security contact to help prepare for their upcoming National Security Information (NSI) inspection. The briefing will cover any security question/issue that needs to be addressed by the bureau/unit prior to the arrival of the inspection team.

2. A tentative date will be scheduled for the NSI inspection. A confirmation date shall be set within two working days following the briefing. The security contact should coordinate this date with management and all key individuals involved in the handling and safeguarding of NSI. Once a confirmation date is made, a letter will be sent to the bureau/unit to restate the purpose of the inspection, points of contacts, and date(s) of visit.

B. The Day of the NSI Inspection. On the day of the NSI inspection, the following personnel should be available throughout the inspection.

1. Bureau/Operating Unit Security Contact.

2. Primary Custodian of each classified container. Any classified handler who is not identified as a custodian should also be made available for the inspection. This is a cleared individual who works directly with the NSI being stored in the container.

3. Alternate Custodian of each classified container in the absence of a custodian. The alternate should be familiar with the contents of the container and be able to open the container.

4. Classified Control Point. The cleared individual responsible for handling incoming and outgoing classified materials.

C. Protection of National Security Information.

1. National Security Information (NSI) is official information that relates to national defense or foreign relations and is the property of the U.S. Government. It is also known as classified information. There are three levels of NSI.

a. Top Secret: applies to information that reasonably could be expected to cause exceptionally grave damage to national security if disclosed to unauthorized sources.

b. Secret: applies only to information that reasonably could be expected to cause serious damage to national security if disclosed to unauthorized sources.

c. Confidential: applies only to information that reasonably could be expected to cause damage to the national security if disclosed to unauthorized sources.

2. If classified information becomes compromised, our nation's advantage would or could be damaged, minimized, or lost, thereby adversely affecting the national security. NSI must be protected with an additional degree of security at all times in order to prevent any unauthorized disclosure.

D. Security Containers.

1. Security containers must be GSA-approved if used for the storage of classified information at the Confidential and/or Secret level. A GSA-approved security container is a metal safe having a built-in, three-position tumbler combination lock. Top Secret information must be stored in a GSA-approved security container as well, but must also be housed in an area that is alarmed and has a 24-hour guard service or response force.

2. Each approved security containers must have a GSA-approved identification plate affixed to it. The GSA-approved identification plate is usually located on the outer top drawer of the container. If a container does not bear this plate, immediately notify the security contact, as the container may not be authorized to store classified information. If you have any questions regarding security containers,

contact your security contact.

3. File cabinets with security bar-locks, known as "bar-lock containers," are no longer approved for the storage of classified information with the following exception. Offices that are currently using bar-lock containers may continue to use them to store material up to the Secret level until the year 2012. (This applies only to those bar-lock containers that have had continuous use prior to the implementation of Executive Order 12958). However, the use of these containers is discouraged.

4. Approved and accredited strongrooms and vaults can be used for open storage of Confidential and Secret information. Secret information must be stored in a facility that has a 24-hour guard service or response force.

5. Each container in an office should be listed in an electronic database, if practicable, identifying the classified contents and the names of all individuals with authorized access to the container. If it is not cost-effective to maintain this information in an electronic data base, it may be maintained in written format. A copy of this document shall be provided to the servicing security officer.

E. Security Container Contents. The following forms must contain up-to-date information and be affixed to the security container:

1. **Form SF-700, Security Container Information.** This form is referred to as the "combination change envelope." Part one of the form must be attached to the inside of the control drawer (or top drawer of a bar-lock container) of approved containers used to store classified information. This form identifies all persons responsible for the container and holds the classified combination. Parts 2 and 2a of Form SF-700 shall be marked accordingly and protected in the same manner as the highest level of classified material stored within the container. When a Form SF-700 contains Secret and Top Secret combinations it shall be properly accounted for. Within the Department of Commerce, the classified envelope shall be forwarded to and retained by either the bureau/unit security contact or the servicing security officer.

2. **Form SF-701, Activity Security Checklist.** Each office/area where classified information is stored and/or processed requires a Form SF- 701, Activity Security Checklist. The office head or security contact shall establish a system of security checks to be conducted at the close of each working day utilizing the SF-701. The end-of-day check acts as a secondary check, an added measure of security required to ensure offices have properly stored classified information at the end of each workday.

3. **Form SF-702, Security Container Check Sheet.** The Form SF-702 must be placed on the

outside of any GSA-approved container that is used for the storage of classified information. The person who opens, closes, and checks the security container must annotate the SF-702. It is recommended that the office retain each completed form for 90 days.

4. **OPEN/CLOSED Sign**. Reversible OPEN/CLOSED signs, or similar signs, shall be used as a reminder on all GSA-approved security containers used for the storage of classified information. They shall be used each time the container is opened or closed. It is vital that each custodian, alternate and individual responsible for the end-of-day security checks ensures that the security container is locked, whether or not the OPEN/CLOSED sign indicates the container is closed. The CLOSED sign is not an indicator that the safe has been properly secured.

5. **Electronic Database System.** All Secret and Top Secret information must be accounted for using either a written or an electronic (where practicable) document tracking system such as the Department's Security Information Management System (SIMS). Annual inventories and Records of Destruction should be recorded using the same system.

F. Security Container Preparation. Proper preparation for a NSI inspection includes a "Clean Out." A thorough "Clean Out" must be conducted, in the following manner.

1. Prepare an accountability record of each container in your bureau/unit, using the Office of Security's electronic database system and compare the documents listed on the report with a physical inventory of those found in the container.

2. Determine if you have a continuous use or need for each classified document stored in the security container.

3. Review all classified holdings for possible downgrading or declassification under E.O. 12958.

4. Ensure that all classified materials (documents, diskettes, etc.) being retained have the appropriate classified cover sheets attached.

5. Ensure that all classified materials being retained in the security container are properly marked.

6. Ensure that all Secret/Top Secret materials stored in the container for retention are recorded in the Office of Security's electronic database system. When the OSY's database system is inoperable, Form CD-481 shall be used. When OSY's database system becomes operable, all items on the Form CD-481 should be transferred to the electronic database EDS.

7. Ensure that all Secret/Top Secret materials selected for destruction are recorded in OSY's electronic database system and protected in a classified "FOR CLASSIFIED WASTE ONLY" burn bag. All classified material selected for destruction in burn bag(s) must be stored in a security container until such time they can be transferred to the Classified Burn Room or shredded by an approved crosscut shredder.

Note: If a determination is made on the day of the NSI inspection that the bureau/unit being inspected did not conduct a thorough "clean out" of its classified security containers, the inspection will be terminated at that point. The security contact and management will be notified and the inspection will be postponed.

G. Review of Classified Documents for Marking.

1. All classified documents must be marked appropriately. Marking instructions and guidance can be found in Chapter 20, Marking, of the manual. All classified documents shall be marked:

- Top and bottom with the appropriate classification level.
- Each subject line identified with the appropriate classification level.
- The beginning of each paragraph must be marked with the appropriate classification level.
- Each classified diagram, map, drawing, etc., must be appropriately marked.
- All classified documents must have declassification instructions located at the bottom of the first page of the document.

2. E.O. 12958, Section 1.8, references classification challenges of improperly marked documents, which have been received by other agencies. The recipient must notify agencies that have sent an improperly marked document that the document was improperly marked. It is not the responsibility of the receiver to correct these mismarkings.

H. Classified Working Papers.

Classified working papers are drafts, notes, photographs, etc. used to create or assist in the preparation of a final document. They must be:

- Dated and signed when created.
- Marked with the highest classification level of the information that they contain.
- Protected in accordance with the assigned classification.

- Properly destroyed when no longer needed
- Accounted for and controlled if transmitted, permanently filed, or retained after 180 days. After 180 days, the document is no longer considered a working paper.

I. Cover Sheets.

All classified and sensitive information (documents and files) stored in a classified security container should have the appropriate cover sheet attached to the front of each document or attached to the cover of each file. If a document is removed from within a file, a cover sheet must be attached to the front of the document. Sensitive cover sheets, Form CD-494 (gray border), established for "Sensitive But Unclassified" (SBU), "For Official Use Only" (FOUO), and other sensitive or administratively controlled information, are used throughout the Department of Commerce.

- Form SF-703 Top Secret (Orange Border)
- Form SF-704 Secret (Red Border)
- Form SF-705 Confidential (Blue Border)
- Form CD-494 Sensitive (Gray Border)

J. Classified Information Systems Processing Magnetic Media.

Information Systems (IS) media, removable magnetic Central Processing Unit (CPU) hard drives, diskettes, tape reels, laser optical compact disks (CD-ROMS) or any other digital media that contain classified information shall be marked with the highest classification of the information contained within the media as follows:

- Form SF-706 Top Secret
- Form SF-707 Secret
- Form SF-708 Confidential

K. Things That Should Not Be Stored with Classified Information.

GSA-approved security containers are intended for the storage of classified information. Classified information must not be stored with:

- Firearms/ammunition
- Money
- Precious metals
- Personal items
  - Purses
  - Radios
  - Jewelry

L. What to Expect after the NSI Inspection.

The Office of Security will provide a written report of all findings and recommendations to the head of an operating unit with a copy to the security contact. A follow-up inspection will be required within six months if serious discrepancies and/or violations are discovered. The decision to conduct a follow-up inspection is determined on a case-by-case basis. The follow-up inspection may be scheduled or unannounced.

M. Frequently Asked Questions/Answers.

Q1: How long does a NSI Inspection take?

A: This is determined by the volume of NSI stored and processed in each bureau/unit, as well as the current NSI management practices in each bureau/unit.

Q2: If a security contact or custodian cannot be available for the inspection, will this pose a problem for the inspection team?

A: Security contacts and all security container custodians are requested to be available throughout the inspection process. If a security contact cannot be present, it is recommended that a back-up person, familiar with the NSI program be available. Any custodian that is unavailable must have an alternate available for the inspection. This alternate must be able to perform all duties of the custodian, to include opening containers.

Q3: What is a Classified Control Point (CCP)?

A: A CCP is a cleared individual who is responsible for the accountability and control of National Security Information in an electronic database for an operating unit or an office. This individual(s) receives, transmits, records, distributes, and may prepare classified documents for destruction. Management of the classified information by the CCP is conducted through the use of the Office of Security's electronic database system.

Q4: Will questions arise pertaining to the technical contents of each classified document?

A: When reviewing documents, the team will address whether any particular document in question needs to be retained. The team will be looking at document dates and asking if these documents have been reviewed for possible downgrading or declassification. Security container custodians are required to be available for this review if the custodian is responsible for the processing of this classified information. If another individual is responsible for the classified information, and is not the custodian of the container, that individual is required to be available for questions.

Q5: Why is the Office of Security conducting NSI inspections at this time?

A: It is the responsibility of the Office of Security to provide security oversight to ensure NSI is being properly handled, stored, and accounted for and that each bureau/operating unit is in compliance with the Department's security regulations.

Q6: I am aware that a NSI inspection will be conducted in my area, but I have several questions that my security contact could not answer. Will the inspection team be available to answer my questions before the inspection?

A: Absolutely; the team will be available to answer these questions during the pre-inspection brief. The team recommends that if a security contact cannot answer relevant security-related questions, you may contact the Office of Security, (202) 482-8115, prior to the inspection for any needed guidance.

Q7: Will the NSI inspections result in anyone losing their security clearance?

A: No. The Office of Security periodically conducts an on-going review of personnel security clearances to determine whether a continued need to retain a clearance is required for each position. If it is determined that an employee does not access any classified information in the performance of his/her official duties, the clearance may be administratively withdrawn. However, this is not accomplished as a part of the NSI inspection visit.

*** * * * * * * * * ***

I.3 U.S. DEPARTMENT OF COMMERCE, OFFICE OF SECURITY, NATIONAL SECURITY INFORMATION CHECK LIST

Bureau Inspected:

Office being inspected:
Room:

Date of inspection:

Inspection team member:

Start time:

End time:

Custodian:
Clearance Level:
Telephone:

(Alt) Custodian:
Clearance Level:
Telephone:

SIMS Control Point:

Highest Level of Classified stored: **TS** **S** **C**

Container identification number:

Type of container:
Number of drawers:

Notes:

Appendix I – National Security Information Check List – Page 2

Y N Have you had an information security inspection? If yes, when?
Does the unit have a copy of the report?

Y N Have the discrepancies noted during the last inspection been corrected?

- - When was your last National Security Information Briefing? _____
Who provided the briefing? _____

Y N Do you understand the purpose of the Office of Security's electronic database?

Y N Do you know who your control point is?

Y N Are there office procedures for the handling and processing of National Security Information?

- - What is the total number of security containers under the control of the custodian being interviewed? _____

Y N Is classified material stored in a GSA-approved security container?

Y N Are all the documents in the container recorded in the Security Information Management Systems (SIMS) or other electronic database system? If no, explain.

Y N Can classified material in the container be promptly located from control records on hand?
If no, explain.

Y N Are appropriate forms being used?
SF-700____ SF-701____ SF-702____

Appendix I – National Security Information Check List – Page 3

Y N Are security container combinations recorded, marked, and stored properly?

Y N Has the security officer initiated procedures to control the reproduction of classified material?

Y N Is the reproduction of classified limited to operational necessity?

Y N When Secret or Top Secret Information is copied, are the additional copies introduced into the accountability system?

Y N Has the copy machine been approved by security for classified usage?

Y N Does the facility have a 24-hour guard force operation?

Y N Before an individual has access to classified information, has his/her clearance and need to know been verified by security?

Y N Is classified information correctly prepared for transmission and noted in SIMS?

Y N Have procedures been established to prevent unauthorized disclosure (visitor control)?

Y N Are the Standard Forms 704, 705, and 706 classified information cover sheets used for internal transmission of classified information?

Y N Does the agency have any Original Classification Authorities?
If yes, who and how many?

Y N Are folders, files, working papers, transmittal documents containing classified information properly marked? (i.e., top and bottom marked to highest classification, portion marking)?

Appendix I – National Security Information Check List – Page 4

Y N Is there an annual inventory of classified documents?

Y N Are there any documents requiring declassification under the E.O. 12968?

Y N Are classified documents held to an absolute minimum?

Y N Are classified documents destroyed? If so how? Shredder_____ Burn Bag_____

Y N If a shredder is used, is it approved and accredited for classified destruction?

Y N Is the destruction of classified documents noted in SIMS or another electronic database?

Y N Does the operating unit use or possess a STU phone?

Y N If yes, has the custodian been designated in writing and properly briefed?

Y N If classified is lost or possible compromise has occurred, what procedures would you take?

Y N SIMS Control Point Question: Are individuals who depart, debriefed, and made aware of their classified accountability?

Y N Have there been any reported security violations?

* * * * * * * * * *